WHAT IS CLAIMED IS:

1. A secure parameter generating device in an algebraic curve cryptography, comprising:

an input means for receiving two different prime numbers (a, b) specifying degree of complexity of a curve and size (n) of an encryption key to be used;

a Stickelberger element computing device for computing a Stickelberger element (ω) in an ab cyclotomic, based on the prime number (a) and the prime number (b);

a Jacobian addition candidate value computing device for computing Jacobian addition candidate value j corresponding to the two different prime numbers a and b, and a prime number p corresponding to the Jacobian addition candidate value j, based on the prime number (a), the prime number (b), the size (n) of an encryption key, and the Stickelberger element (ω) ;

an order candidate value computing device for computing a class H consisting of a plurality of candidate values for order of a Jacobian group of an algebraic curve specified by the prime number a and the prime number b, based on the prime number a, the prime number b, and the Jacobian addition candidate value j;

a security judging device for searching for a candidate value h meeting a security condition such as almost prime number characteristic from the class H,

according to the class H;

a parameter deciding device for computing a parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a, the prime number b, and the prime number p, based on the prime number a, the prime number b, the prime number p, and the candidate value h; and

an output device for supplying the parameter of the algebraic curve computed by said parameter deciding device.

2. A secure parameter generating device in an algebraic curve cryptography as claimed in Claim 1, further comprising:

an a-storing means, a b-storing means, and an n-storing means for respectively storing the prime number a, the prime number b, and the size n of the encryption key received by said input means;

a ω-storing means for storing a Stickelberger element ω computed by said Stickelberger element computing device;

a p-storing means and a j-storing means for respectively storing the prime number p and the Jacobian addition candidate value j computed by said Jacobian addition candidate value computing device;

an H-storing means for storing the class H

computed by said order candidate value computing device; and

an h-storing means for storing the candidate value h found by said security judging device.

3. A secure parameter generating device in an algebraic curve cryptography as claimed in Claim 1, further comprising:

said Stickelberger element computing device for computing the Stickelberger element ω by use of the equation $\omega = \Sigma_t$ [<t/a> + <t/b>] $\sigma\_\{-t^{-1}\}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, [λ] indicates the maximum integer not exceeding a rational number λ, <λ> indicates a fractional portion λ-[λ] of the rational number λ, σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b.

4. A secure parameter generating device in an algebraic curve cryptography as claimed in Claim 1, further comprising:

said Jacobian addition candidate value computing device for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length

2n/(a-1)(b-1) or so, based on the prime number a, the prime number b, the size n of the encryption key, and the Stickelberger element ω, and computing the Jacobian addition candidate value j by use of the equation $j = \gamma^{\omega}$.

5. A secure parameter generating device in an algebraic curve cryptography as claimed in Claim 1, further comprising:

said Stickelberger element computing device for computing the Stickelberger element ω by use of the equation $\omega = \Sigma_t$ [<t/a> + <t/b>] $\sigma_{-t^{-1}}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, [λ] indicates the maximum integer not exceeding a rational number λ, <λ> indicates a fractional portion λ-[λ] of the rational number λ, σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b; and

said Jacobian addition candidate value computing device for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length 2n/(a-1)(b-1) or so, based on the prime number a, the prime number b, the size n of the encryption key, and the Stickelberger element ω, and computing the

Jacobian addition candidate value j by use of the equation $j = \gamma^{\omega}$.

6. A secure parameter generating device in an algebraic curve cryptography as claimed in Claim 1, further comprising:

said order candidate value computing device for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the parameters a and b, using the equation $h_k = \mathrm{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where Norm_{K|Q} is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to 2ab inclusively, when ζ is the primitive ab root of 1, based on the prime number a, the prime number b, and the Jacobian addition candidate value j, and computing the class of the candidate values, $H=\{h_1, h_2, \cdots, h_{2ab}\}$.

7. A secure parameter generating device in an algebraic curve cryptography as claimed in Claim 1, further comprising:

said Stickelberger element computing device for computing the Stickelberger element ω by use of the equation $\omega = \Sigma_t [<t/a> + <t/b>] \sigma_{-t^{-1}}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, $[\lambda]$ indicates the maximum integer not exceeding a rational number λ, $<\lambda>$ indicates a fractional portion $\lambda - [\lambda]$ of the rational number λ, σ_t

indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b; and

said order candidate value computing device for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the parameters a and b, using the equation $h_k = \mathrm{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where Norm_{K|Q} is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to 2ab inclusively, when ζ is the primitive ab root of 1, based on the prime number a, the prime number b, and the Jacobian addition candidate value j, and computing the class of the candidate values, $H=\{h_1, h_2, \cdots, h_{2ab}\}$.

8. A secure parameter generating device in an algebraic curve cryptography as claimed in Claim 1, further comprising:

said Jacobian addition candidate value computing device for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length 2n/(a-1)(b-1) or so, based on the prime number a, the prime number b, the size n of the encryption key, and the Stickelberger element ω, and computing the Jacobian addition candidate value j by use of the equation $j = \gamma^{\omega}$; and

said order candidate value computing device for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the parameters a and b, using the equation $h_k = \mathrm{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where Norm_{K|Q} is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to 2ab inclusively, when ζ is the primitive ab root of 1, based on the prime number a, the prime number b, and the Jacobian addition candidate value j, and computing the class of the candidate values, $H=\{h_1,h_2,\cdots,h_{2ab}\}$.

9. A secure parameter generating device in an algebraic curve cryptography as claimed in Claim 1, further comprising:

said Stickelberger element computing device for computing the Stickelberger element ω by use of the equation $\omega = \Sigma_t [<t/a> + <t/b>] \sigma_{-t^{-1}}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, $[\lambda]$ indicates the maximum integer not exceeding a rational number λ, $<\lambda>$ indicates a fractional portion $\lambda-[\lambda]$ of the rational number λ, σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b;

said Jacobian addition candidate value computing device for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K

generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length 2n/(a-1)(b-1) or so, based on the prime number a, the prime number b, the size n of the encryption key, and the Stickelberger element ω, and computing the Jacobian addition candidate value j by use of the equation $j = \gamma^{\omega}$; and

said order candidate value computing device for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the parameters a and b, using the equation $h_k = \mathrm{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where Norm_{K|Q} is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to 2ab inclusively, when ζ is the primitive ab root of 1, based on the prime number a, the prime number b, and the Jacobian addition candidate value j, and computing the class of the candidate values, $H=\{h_1, h_2, \cdots, h_{2ab}\}$.

10. A secure parameter generating device in an algebraic curve cryptography as claimed in Claim 1, further comprising:

said parameter deciding device for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on the prime number a, the prime number b, the prime number p, and the candidate value h, generating a random point G over an algebraic curve defined by the equation $\zeta_a^1 Y^a$

+ $\zeta_b^m X^b + 1 = 0$, as for each integer 1 from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h-fold of an element in the Jacobian group indicated by the point G, and supplying p, ζ_a^1, and ζ_b^m as the parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

11. A secure parameter generating device in an algebraic curve cryptography as claimed in Claim 1, further comprising:

said Stickelberger element computing device for computing the Stickelberger element ω by use of the equation $\omega = \Sigma_t$ [<t/a> + <t/b>] $\sigma_{-t^{-1}}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, [λ] indicates the maximum integer not exceeding a rational number λ, <λ> indicates a fractional portion λ-[λ] of the rational number λ, σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b; and

said parameter deciding device for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on the prime number a, the prime number b, the prime number

p, and the candidate value h, generating a random point G over an algebraic curve defined by the equation $\zeta_a^l Y^a + \zeta_b^m X^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h-fold of an element in the Jacobian group indicated by the point G, and supplying p, ζ_a^l, and ζ_b^m as the parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

12. A secure parameter generating device in an algebraic curve cryptography as claimed in Claim 1, further comprising:

said Jacobian addition candidate value computing device for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length 2n/(a-1)(b-1) or so, based on the prime number a, the prime number b, the size n of the encryption key, and the Stickelberger element ω, and computing the Jacobian addition candidate value j by use of the equation $j = \gamma^{\omega}$; and

said parameter deciding device for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1

with the prime number p used as the divisor, based on the prime number a, the prime number b, the prime number p, and the candidate value h, generating a random point G over an algebraic curve defined by the equation $\zeta_a^l Y^a + \zeta_b^m X^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h-fold of an element in the Jacobian group indicated by the point G, and supplying p, ζ_a^l, and ζ_b^m as the parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

13. A secure parameter generating device in an algebraic curve cryptography as claimed in Claim 1, further comprising:

said order candidate value computing device for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the parameters a and b, using the equation $h_k = \mathrm{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where Norm_{K|Q} is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to 2ab inclusively, when ζ is the primitive ab root of 1, based on the prime number a, the prime number b, and the Jacobian addition candidate value j, and computing the class of the candidate values, $H=\{h_1, h_2, \ldots, h_{2ab}\}$; and

said parameter deciding device for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on the prime number a, the prime number b, the prime number p, and the candidate value h, generating a random point G over an algebraic curve defined by the equation $\zeta_a^{\,l}\, Y^a + \zeta_b^{\,m}\, X^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h-fold of an element in the Jacobian group indicated by the point G, and supplying p, $\zeta_a^{\,l}$, and $\zeta_b^{\,m}$ as the parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

14. A secure parameter generating device in an algebraic curve cryptography as claimed in Claim 1, further comprising:

said Stickelberger element computing device for computing the Stickelberger element ω by use of the equation $\omega = \Sigma_t\, [<t/a> + <t/b>]\, \sigma\_\{-t^{-1}\}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, $[\lambda]$ indicates the maximum integer not exceeding a rational number λ, $<\lambda>$ indicates a fractional portion $\lambda - [\lambda]$ of the rational number λ, σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic

(ζ is the primitive ab root of 1)), based on the prime number a and the prime number b;

said Jacobian addition candidate value computing device for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length 2n/(a-1)(b-1) or so, based on the prime number a, the prime number b, the size n of the encryption key, and the Stickelberger element ω, and computing the Jacobian addition candidate value j by use of the equation $j = \gamma^{\omega}$; and

said parameter deciding device for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on the prime number a, the prime number b, the prime number p, and the candidate value h, generating a random point G over an algebraic curve defined by the equation $\zeta_a^{l} Y^a + \zeta_b^{m} X^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h-fold of an element in the Jacobian group indicated by the point G, and supplying p, ζ_a^{l}, and ζ_b^{m} as the parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

15. A secure parameter generating device in an algebraic curve cryptography as claimed in Claim 1, further comprising:

said Stickelberger element computing device for computing the Stickelberger element ω by use of the equation $\omega = \Sigma_t$ [<t/a> + <t/b>] $\sigma_{-t^{-1}}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, [λ] indicates the maximum integer not exceeding a rational number λ, <λ> indicates a fractional portion λ-[λ] of the rational number λ, σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b;

said order candidate value computing device for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the parameters a and b, using the equation $h_k = \mathrm{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where $\mathrm{Norm}_{K|Q}$ is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to 2ab inclusively, when ζ is the primitive ab root of 1, based on the prime number a, the prime number b, and the Jacobian addition candidate value j, and computing the class of the candidate values, $H=\{h_1,h_2,\cdots,h_{2ab}\}$; and

said parameter deciding device for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on

the prime number a, the prime number b, the prime number p, and the candidate value h, generating a random point G over an algebraic curve defined by the equation $\zeta_a^{\,l}\, Y^a + \zeta_b^{\,m}\, X^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h-fold of an element in the Jacobian group indicated by the point G, and supplying p, $\zeta_a^{\,l}$, and $\zeta_b^{\,m}$ as the parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

16. A secure parameter generating device in an algebraic curve cryptography as claimed in Claim 1, further comprising:

said Jacobian addition candidate value computing device for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length 2n/(a-1)(b-1) or so, based on the prime number a, the prime number b, the size n of the encryption key, and the Stickelberger element ω, and computing the Jacobian addition candidate value j by use of the equation $j = \gamma^{\omega}$;

said order candidate value computing device for

computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the parameters a and b, using the equation $h_k = \mathrm{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where Norm_{K|Q} is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to 2ab inclusively, when ζ is the primitive ab root of 1, based on the prime number a, the prime number b, and the Jacobian addition candidate value j, and computing the class of the candidate values, $H=\{h_1, h_2, \ldots, h_{2ab}\}$; and

said parameter deciding device for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on the prime number a, the prime number b, the prime number p, and the candidate value h, generating a random point G over an algebraic curve defined by the equation $\zeta_a^l Y^a + \zeta_b^m X^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h-fold of an element in the Jacobian group indicated by the point G, and supplying p, ζ_a^l, and ζ_b^m as the parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

17. A secure parameter generating device in an algebraic curve cryptography as claimed in Claim 1,

further comprising:

said Stickelberger element computing device for computing the Stickelberger element ω by use of the equation $\omega = \Sigma_t [<t/a> + <t/b>] \sigma_{-t^{-1}}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, $[\lambda]$ indicates the maximum integer not exceeding a rational number λ, $<\lambda>$ indicates a fractional portion $\lambda-[\lambda]$ of the rational number λ, σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b;

said Jacobian addition candidate value computing device for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length 2n/(a-1)(b-1) or so, based on the prime number a, the prime number b, the size n of the encryption key, and the Stickelberger element ω, and computing the Jacobian addition candidate value j by use of the equation $j = \gamma^{\omega}$;

said order candidate value computing device for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the parameters a and b, using the equation $h_k = \mathrm{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where Norm_{K|Q} is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1

to 2ab inclusively, when ζ is the primitive ab root of 1, based on the prime number a, the prime number b, and the Jacobian addition candidate value j, and computing the class of the candidate values, $H=\{h_1,h_2,\cdots,h_{2ab}\}$; and

said parameter deciding device for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on the prime number a, the prime number b, the prime number p, and the candidate value h, generating a random point G over an algebraic curve defined by the equation $\zeta_a^{\,l}\,Y^a + \zeta_b^{\,m}\,X^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h-fold of an element in the Jacobian group indicated by the point G, and supplying p, $\zeta_a^{\,l}$, and $\zeta_b^{\,m}$ as the parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

18. A secure parameter generating method in an algebraic curve, comprising the steps of:

a Stickelberger element computing procedure for computing a Stickelberger element ω in an ab cyclotomic, respectively based on two different prime numbers a and b specifying degree of complexity of curve;

a Jacobian addition candidate value computing

procedure for computing Jacobian addition candidate value j corresponding to the two different prime numbers a and b, and a prime number p corresponding to the Jacobian addition candidate value j, respectively based on the prime number a, the prime number b, the size n of an encryption key, and the Stickelberger element ω;

an order candidate value computing procedure for computing a class H consisting of a plurality of candidate values for order of a Jacobian group of an algebraic curve specified by the prime number a and the prime number b, respectively based on the prime number a, the prime number b, and the Jacobian addition candidate value j;

a security judging procedure for searching for a candidate value h meeting a security condition such as almost prime number characteristic from the class H, according to the class H; and

a parameter deciding procedure for computing a parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a, the prime number b, and the prime number p, respectively based on the prime number a, the prime number b, the prime number p, and the candidate value h.

19. A secure parameter generating method in an algebraic curve cryptography as claimed in Claim 18,

further comprising:

a procedure for storing a Stickelberger element ω computed by said Stickelberger element computing procedure into said ω-storing means;

a procedure for respectively storing the prime number p and the Jacobian addition candidate value j computed by said Jacobian addition candidate value computing procedure into said p-storing means and j-storing means;

a procedure for storing the class H computed by said order candidate value computing procedure into said H-storing means; and

a procedure for storing the candidate value h found by said security judging procedure into said h-storing means.

20. A secure parameter generating method in an algebraic curve cryptography as claimed in Claim 18, further comprising:

said Stickelberger element computing procedure for computing the Stickelberger element ω by use of the equation $\omega = \Sigma_t$ [<t/a> + <t/b>] $\sigma\_\{-t^{-1}\}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, [λ] indicates the maximum integer not exceeding a rational number λ, <λ> indicates a fractional portion λ-[λ] of the rational number λ, σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic

(ζ is the primitive ab root of 1)), based on the prime number a and the prime number b.

21. A secure parameter generating method in an algebraic curve cryptography as claimed in Claim 18, further comprising:

said Jacobian addition candidate value computing procedure for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length 2n/(a-1)(b-1) or so, based on the prime number a, the prime number b, the size n of the encryption key, and the Stickelberger element ω, and computing the Jacobian addition candidate value j by use of the equation $j = \gamma^{\omega}$.

22. A secure parameter generating method in an algebraic curve cryptography as claimed in Claim 18, further comprising:

said Stickelberger element computing procedure for computing the Stickelberger element ω by use of the equation $\omega = \Sigma_t$ [<t/a> + <t/b>] $\sigma\_\{-t^{-1}\}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, [λ] indicates the maximum integer not exceeding a rational number λ, <λ> indicates a fractional portion λ-[λ] of the rational number λ, σ_t

indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b; and

said Jacobian addition candidate value computing procedure for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length 2n/(a-1)(b-1) or so, based on the prime number a, the prime number b, the size n of the encryption key, and the Stickelberger element ω, and computing the Jacobian addition candidate value j by use of the equation $j = \gamma^{\omega}$.

23. A secure parameter generating method in an algebraic curve cryptography as claimed in Claim 18, further comprising:

said order candidate value computing procedure for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the parameters a and b, using the equation $h_k = \mathrm{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where Norm_{K|Q} is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to 2ab inclusively, when ζ is the primitive ab root of 1, based on the prime number a, the prime number b, and the Jacobian addition candidate value j, and computing the class of the candidate values, $H=\{h_1, h_2, \cdots, h_{2ab}\}$.

24. A secure parameter generating method in an algebraic curve cryptography as claimed in Claim 18, further comprising:

said Stickelberger element computing procedure for computing the Stickelberger element ω by use of the equation $\omega = \Sigma_t$ [<t/a> + <t/b>] $\sigma_{-t^{-1}}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, [λ] indicates the maximum integer not exceeding a rational number λ, <λ> indicates a fractional portion λ-[λ] of the rational number λ, σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b; and

said order candidate value computing procedure for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the parameters a and b, using the equation $h_k = \mathrm{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where $\mathrm{Norm}_{K|Q}$ is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to 2ab inclusively, when ζ is the primitive ab root of 1, based on the prime number a, the prime number b, and the Jacobian addition candidate value j, and computing the class of the candidate values, $H=\{h_1, h_2, \cdots, h_{2ab}\}$.

25. A secure parameter generating method in an algebraic curve cryptography as claimed in Claim 18,

further comprising:

said Jacobian addition candidate value computing procedure for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length 2n/(a-1)(b-1) or so, based on the prime number a, the prime number b, the size n of the encryption key, and the Stickelberger element ω, and computing the Jacobian addition candidate value j by use of the equation $j = \gamma^{\omega}$; and

said order candidate value computing procedure for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the parameters a and b, using the equation $h_k = Norm_{K|Q}(1 + (-\zeta)^k j)$ (where Norm_{K|Q} is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to 2ab inclusively, when ζ is the primitive ab root of 1, based on the prime number a, the prime number b, and the Jacobian addition candidate value j, and computing the class of the candidate values, $H=\{h_1, h_2, \cdots, h_{2ab}\}$.

26. A secure parameter generating method in an algebraic curve cryptography as claimed in Claim 18, further comprising:

said Stickelberger element computing procedure for computing the Stickelberger element ω by use of the

equation $\omega = \Sigma t\ [<t/a> + <t/b>]\ \sigma_{-t-1}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, $[\lambda]$ indicates the maximum integer not exceeding a rational number λ, $<\lambda>$ indicates a fractional portion $\lambda-[\lambda]$ of the rational number λ, σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b;

said Jacobian addition candidate value computing procedure for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length 2n/(a-1)(b-1) or so, based on the prime number a, the prime number b, the size n of the encryption key, and the Stickelberger element ω, and computing the Jacobian addition candidate value j by use of the equation $j = \gamma^{\omega}$; and

said order candidate value computing procedure for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the parameters a and b, using the equation $h_k = \mathrm{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where $\mathrm{Norm}_{K|Q}$ is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to 2ab inclusively, when ζ is the primitive ab root of 1, based on the prime number a, the prime number b, and the Jacobian addition candidate value j, and computing the

class of the candidate values, $H=\{h_1, h_2, \cdots, h_{2ab}\}$.

27. A secure parameter generating method in an algebraic curve cryptography as claimed in Claim 18, further comprising:

said parameter deciding procedure for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on the prime number a, the prime number b, the prime number p, and the candidate value h, generating a random point G over an algebraic curve defined by the equation $\zeta_a^{\,l}\, Y^a + \zeta_b^{\,m}\, X^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h-fold of an element in the Jacobian group indicated by the point G, and supplying p, $\zeta_a^{\,l}$, and $\zeta_b^{\,m}$ as the parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

28. A secure parameter generating method in an algebraic curve cryptography as claimed in Claim 18, further comprising:

said Stickelberger element computing procedure for computing the Stickelberger element ω by use of the equation $\omega = \Sigma_t\, [<t/a> + <t/b>]\, \sigma_{-t^{-1}}$ (where, t runs

on a typical series of irreducible residue class with ab used as a divisor, $[\lambda]$ indicates the maximum integer not exceeding a rational number λ, $<\lambda>$ indicates a fractional portion $\lambda-[\lambda]$ of the rational number λ, σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b; and

said parameter deciding procedure for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on the prime number a, the prime number b, the prime number p, and the candidate value h, generating a random point G over an algebraic curve defined by the equation $\zeta_a^{\,l}\, Y^a + \zeta_b^{\,m}\, X^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h-fold of an element in the Jacobian group indicated by the point G, and supplying p, $\zeta_a^{\,l}$, and $\zeta_b^{\,m}$ as the parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

29. A secure parameter generating method in an algebraic curve cryptography as claimed in Claim 18, further comprising:

said Jacobian addition candidate value computing

procedure for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length 2n/(a-1)(b-1) or so, based on the prime number a, the prime number b, the size n of the encryption key, and the Stickelberger element ω, and computing the Jacobian addition candidate value j by use of the equation $j = \gamma^{\omega}$; and

said parameter deciding procedure for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on the prime number a, the prime number b, the prime number p, and the candidate value h, generating a random point G over an algebraic curve defined by the equation $\zeta_a^{l} Y^a + \zeta_b^{m} X_b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h-fold of an element in the Jacobian group indicated by the point G, and supplying p, ζ_a^{l}, and ζ_b^{m} as the parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

30. A secure parameter generating method in an algebraic curve cryptography as claimed in Claim 18,

further comprising:

said order candidate value computing procedure for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the parameters a and b, using the equation $h_k = Norm_{K|Q}(1 + (-\zeta)^k j)$ (where Norm_{K|Q} is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to 2ab inclusively, when ζ is the primitive ab root of 1, based on the prime number a, the prime number b, and the Jacobian addition candidate value j, and computing the class of the candidate values, $H=\{h_1, h_2, \ldots, h_{2ab}\}$; and

said parameter deciding procedure for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on the prime number a, the prime number b, the prime number p, and the candidate value h, generating a random point G over an algebraic curve defined by the equation $\zeta_a^l Y^a + \zeta_b^m X^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h-fold of an element in the Jacobian group indicated by the point G, and supplying p, ζ_a^l, and ζ_b^m as the parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

31. A secure parameter generating method in an algebraic curve cryptography as claimed in Claim 18, further comprising:

said Stickelberger element computing procedure for computing the Stickelberger element ω by use of the equation $\omega = \Sigma_t$ [<t/a> + <t/b>] $\sigma\_\{-t^{-1}\}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, [λ] indicates the maximum integer not exceeding a rational number λ, <λ> indicates a fractional portion λ-[λ] of the rational number λ, σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b;

said Jacobian addition candidate value computing procedure for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length 2n/(a-1)(b-1) or so, based on the prime number a, the prime number b, the size n of the encryption key, and the Stickelberger element ω, and computing the Jacobian addition candidate value j by use of the equation $j = \gamma^{\omega}$; and

said parameter deciding procedure for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on the prime number a, the prime number b, the prime number

p, and the candidate value h, generating a random point G over an algebraic curve defined by the equation $\zeta_a^l Y^a + \zeta_b^m X^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h-fold of an element in the Jacobian group indicated by the point G, and supplying p, ζ_a^l, and ζ_b^m as the parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

32. A secure parameter generating method in an algebraic curve cryptography as claimed in Claim 18, further comprising:

said Stickelberger element computing procedure for computing the Stickelberger element ω by use of the equation $\omega = \Sigma_t$ [<t/a> + <t/b>] $\sigma\_\{-t^{-1}\}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, [λ] indicates the maximum integer not exceeding a rational number λ, <λ> indicates a fractional portion λ-[λ] of the rational number λ, σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b;

said order candidate value computing procedure for computing a candidate value h_k for the order of the

Jacobian group of an algebraic curve specified by the parameters a and b, using the equation $h_k = Norm_{K|Q}(1 + (-\zeta)^k j)$ (where Norm_{K|Q} is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to 2ab inclusively, when ζ is the primitive ab root of 1, based on the prime number a, the prime number b, and the Jacobian addition candidate value j, and computing the class of the candidate values, $H=\{h_1,h_2,\cdots,h_{2ab}\}$; and

said parameter deciding procedure for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on the prime number a, the prime number b, the prime number p, and the candidate value h, generating a random point G over an algebraic curve defined by the equation $\zeta_a^l Y^a + \zeta_b^m X^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h-fold of an element in the Jacobian group indicated by the point G, and supplying p, ζ_a^l, and ζ_b^m as the parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

33. A secure parameter generating method in an algebraic curve cryptography as claimed in Claim 18, further comprising:

said Jacobian addition candidate value computing procedure for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length 2n/(a-1)(b-1) or so, based on the prime number a, the prime number b, the size n of the encryption key, and the Stickelberger element ω, and computing the Jacobian addition candidate value j by use of the equation $j = \gamma^{\omega}$;

said order candidate value computing procedure for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the parameters a and b, using the equation $h_k = \mathrm{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where Norm_{K|Q} is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to 2ab inclusively, when ζ is the primitive ab root of 1, based on the prime number a, the prime number b, and the Jacobian addition candidate value j, and computing the class of the candidate values, $H=\{h_1, h_2, \cdots, h_{2ab}\}$; and

said parameter deciding procedure for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on the prime number a, the prime number b, the prime number p, and the candidate value h, generating a random point G over an algebraic curve defined by the equation $\zeta_a^{\,l} Y^a + \zeta_b^{\,m} X^b + 1 = 0$, as for each integer l from 1 to a

inclusively and each integer m from 1 to b inclusively, computing the h-fold of an element in the Jacobian group indicated by the point G, and supplying p, ζ_a^1, and ζ_b^m as the parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

34. A secure parameter generating method in an algebraic curve cryptography as claimed in Claim 18, further comprising:

said Stickelberger element computing procedure for computing the Stickelberger element ω by use of the equation $\omega = \Sigma_t$ [<t/a> + <t/b>] $\sigma\_\{-t^{-1}\}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, [λ] indicates the maximum integer not exceeding a rational number λ, <λ> indicates a fractional portion λ-[λ] of the rational number λ, σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b;

said Jacobian addition candidate value computing procedure for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit

length 2n/(a-1)(b-1) or so, based on the prime number a, the prime number b, the size n of the encryption key, and the Stickelberger element ω, and computing the Jacobian addition candidate value j by use of the equation $j = \gamma^{\omega}$;

said order candidate value computing procedure for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the parameters a and b, using the equation $h_k = \mathrm{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where Norm_{K|Q} is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to 2ab inclusively, when ζ is the primitive ab root of 1, based on the prime number a, the prime number b, and the Jacobian addition candidate value j, and computing the class of the candidate values, $H=\{h_1, h_2, \cdots, h_{2ab}\}$; and

said parameter deciding procedure for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on the prime number a, the prime number b, the prime number p, and the candidate value h, generating a random point G over an algebraic curve defined by the equation $\zeta_a^{\,l} Y^a + \zeta_b^{\,m} X^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h-fold of an element in the Jacobian group indicated by the point G, and supplying p, $\zeta_a^{\,l}$, and $\zeta_b^{\,m}$ as the parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value

h, of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.

35. A computer readable memory storing a program for generating a secure parameter in an algebraic curve cryptography, to run the program on a computer,

the program comprising the steps of:

a Stickelberger element computing procedure for computing a Stickelberger element ω in an ab cyclotomic, respectively based on two different prime numbers a and b specifying degree of complexity of curve;

a Jacobian addition candidate value computing procedure for computing Jacobian addition candidate value j corresponding to the two different prime numbers a and b, and a prime number p corresponding to the Jacobian addition candidate value j, respectively based on the prime number a, the prime number b, the size n of an encryption key, and the Stickelberger element ω;

an order candidate value computing procedure for computing a class H consisting of a plurality of candidate values for order of a Jacobian group of an algebraic curve specified by the prime number a and the prime number b, respectively based on the prime number a, the prime number b, and the Jacobian addition candidate value j;

a security judging procedure for searching for a

candidate value h meeting a security condition such as almost prime number characteristic from the class H, according to the class H; and

a parameter deciding procedure for computing a parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a, the prime number b, and the prime number p, respectively based on the prime number a, the prime number b, the prime number p, and the candidate value h.

36. A computer readable memory storing a program for generating a secure parameter in an algebraic curve cryptography,

the program comprising the steps of:

said Stickelberger element computing procedure for computing the Stickelberger element ω by use of the equation $\omega = \Sigma_t$ [<t/a> + <t/b>] $\sigma_{-t^{-1}}$ (where, t runs on a typical series of irreducible residue class with ab used as a divisor, [λ] indicates the maximum integer not exceeding a rational number λ, <λ> indicates a fractional portion λ-[λ] of the rational number λ, σ_t indicates Galois mapping $\zeta \rightarrow \zeta^t$ in the ab cyclotomic (ζ is the primitive ab root of 1)), based on the prime number a and the prime number b.

37. A computer readable memory storing a program for

generating a secure parameter in an algebraic curve cryptography,

the program comprising the steps of:

said Jacobian addition candidate value computing procedure for generating α at random, which is an algebraic integer γ generating a prime ideal of a cyclotomic K generated by the primitive ab root of 1 and whose absolute norm becomes the prime number p of bit length 2n/(a-1)(b-1) or so, based on the prime number a, the prime number b, the size n of the encryption key, and the Stickelberger element ω, and computing the Jacobian addition candidate value j by use of the equation $j = \gamma^{\omega}$.

38. A computer readable memory storing a program for generating a secure parameter in an algebraic curve cryptography,

the program comprising the steps of:

said order candidate value computing procedure for computing a candidate value h_k for the order of the Jacobian group of an algebraic curve specified by the parameters a and b, using the equation $h_k = \mathrm{Norm}_{K|Q}(1 + (-\zeta)^k j)$ (where Norm_{K|Q} is a norm mapping in the ab cyclotomic K), as for each k that is an integer from 1 to 2ab inclusively, when ζ is the primitive ab root of 1, based on the prime number a, the prime number b, and the Jacobian addition candidate value j, and computing the

class of the candidate values, $H=\{h_1, h_2, \ldots, h_{2ab}\}$.

39. A computer readable memory storing a program for generating a secure parameter in an algebraic curve cryptography,

the program comprising the steps of:

said parameter deciding procedure for requiring the primitive a root ζ_a and the primitive b root ζ_b of 1 with the prime number p used as the divisor, based on the prime number a, the prime number b, the prime number p, and the candidate value h, generating a random point G over an algebraic curve defined by the equation $\zeta_a^{\,l}\, Y^a + \zeta_b^{\,m}\, X^b + 1 = 0$, as for each integer l from 1 to a inclusively and each integer m from 1 to b inclusively, computing the h-fold of an element in the Jacobian group indicated by the point G, and supplying p, $\zeta_a^{\,l}$, and $\zeta_b^{\,m}$ as the parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a and the prime number b if the result is equal to an identity element in the Jacobian group.